https://www.linkedin.com/in/joas-antonio-dos-santos/

MALWARE ANALYSIS PYTHON-LIB

1. PyMal: A Python library that provides tools for malware analysis, including functions for extracting static and dynamic features from malware samples.
   - GitHub repository: https://github.com/Neo23x0/pymal
2. YARA: A powerful pattern matching swiss knife for malware researchers. YARA allows you to create custom rules for identifying and classifying malware samples based on patterns and characteristics.
   - GitHub repository: https://github.com/VirusTotal/yara
3. PEFile: A Python library for parsing Portable Executable (PE) files, which are the executable file format used in Windows. PEFile allows you to extract information such as imported and exported functions, sections, headers, and more.
   - GitHub repository: https://github.com/erocarrera/pefile
4. Capstone: A lightweight, multi-platform disassembly framework that can be used for analyzing and reverse engineering malware. It provides a simple and efficient way to disassemble binary files and obtain their assembly instructions.
   - GitHub repository: https://github.com/aquynh/capstone
5. Radare2: A powerful framework for reverse engineering and analyzing binaries. Radare2 provides a wide range of features and tools for disassembling, debugging, analyzing, and modifying executable files, making it useful for malware analysis.
   - Official website: https://radare.org/

FORENSIC ANALYSIS PYTHON-LIB

1. Volatility: A popular framework for memory forensics, Volatility allows you to extract valuable information from memory dumps, such as running processes, network connections, open files, and more.
   - GitHub repository: https://github.com/volatilityfoundation/volatility
2. Autopsy: An open-source digital forensics platform that provides a graphical interface for analyzing disk images. It includes a wide range of built-in modules and supports plugins for extending its functionality.
   - Official website: https://www.autopsy.com/
3. PyTSK: A Python binding for the Sleuth Kit (TSK) library, which is a collection of forensic tools for analyzing disk images. PyTSK provides a high-level interface for working with file systems, partitions, and file metadata.
   - GitHub repository: https://github.com/py4n6/pytsk
4. DFF: Digital Forensics Framework (DFF) is a modular platform that integrates various open-source digital forensics tools. It provides a unified interface for performing forensic analysis on disk images, network captures, and more.
   - Official website: https://www.digital-forensic.org/
5. Plaso: A Python library for creating timelines from various sources of forensic evidence, such as Windows event logs, file system metadata, and more. Plaso simplifies the process of correlating and analyzing events in a timeline format.
   - GitHub repository: https://github.com/log2timeline/plaso

PENTEST PYTHON-LIB

1. Scapy: A powerful interactive packet manipulation program and library that allows you to create, send, and capture network packets. It can be used for various pentesting tasks, such as network reconnaissance, packet sniffing, and more.
   - Official website: https://scapy.net/
2. Metasploit Framework (pymetasploit3): A Python library that provides a programmatic interface to the Metasploit Framework, which is a widely used tool for penetration testing and exploit development. It allows you to automate tasks and interact with Metasploit's features.
   - GitHub repository: https://github.com/allfro/pymetasploit3
3. Requests: A popular Python library for sending HTTP requests and interacting with web services. Requests can be used for various pentesting activities, such as testing web application security vulnerabilities, performing API testing, and more.
   - Official website: https://docs.python-requests.org/
4. Paramiko: A Python library for implementing SSH protocols and managing SSH connections. Paramiko enables you to automate SSH-based tasks, such as remote command execution, file transfers, and more, which are commonly encountered during pentesting engagements.
   - GitHub repository: https://github.com/paramiko/paramiko
5. Impacket: A collection of Python classes for working with network protocols. Impacket allows you to interact with various network protocols and perform tasks like packet crafting, network scanning, password cracking, and more. It is widely used in penetration testing engagements.
   - GitHub repository: https://github.com/SecureAuthCorp/impacket